

ON THE INDICES OF CURVES OVER LOCAL FIELDS

PETE L. CLARK

ABSTRACT. Fix a non-negative integer g and a positive integer I dividing $2g - 2$. For any Henselian, discretely valued field K whose residue field is perfect and admits a degree I cyclic extension, we construct a curve $C_{/K}$ of genus g and index I . This is obtained via a systematic analysis of local points on arithmetic surfaces with semistable reduction. Applications are discussed to the corresponding problem over number fields.

NOTATION AND CONVENTIONS

Throughout this paper K shall denote a field and k a perfect field. We denote by \bar{k} an algebraic closure of k and set $\mathfrak{g}_k = \text{Gal}(\bar{k}/k)$, the absolute Galois group of k . From §2 onwards, K will be Henselian for a discrete valuation v , with valuation ring R and residue field k .

By a variety (resp. a curve) over a field denoted K we will mean a finite-type K -scheme which is smooth, projective and geometrically integral (resp. of dimension one). By a variety (resp. a curve) over a perfect field denoted k we will mean a finite-type k -scheme which is geometrically integral (resp. of dimension one) but possibly incomplete or singular. If V is a variety defined over K and L/K is a field extension, we say that L *splits* V if $V(L) \neq \emptyset$.

1. INTRODUCTION

Given a variety V defined over a field K , one would like to determine whether V has a K -rational point, and if it does not, to say something about $\mathcal{S}(V)$, the set of finite field extensions L/K for which V acquires an L -rational point. This is a very difficult problem: e.g., it is believed by many (but unproved) that there is no algorithm for the task of deciding whether a variety $V_{/\mathbb{Q}}$ has a \mathbb{Q} -rational point.

In order to quantify the second part of the question, we introduce the *index* $I(V)$ of a variety $V_{/K}$: it is the greatest common divisor of all degrees of closed points on V . Equivalently, $I(V)$ is the least positive degree of a K -rational zero-cycle on V . For a curve $C_{/K}$, the index is equal to the least positive degree of a line bundle on $C_{/K}$. If C has genus g , then the canonical bundle $\Omega_{C/K}^1$ has degree equal to $2g - 2$ and $I(C) \mid 2g - 2$.¹

To know $I(V)$ is much less than to know $\mathcal{S}(V)$: we need not know any particular splitting field L/K , nor even the least possible degree of a splitting field (a quantity called the *m-invariant* $m(V)$ in [4]). E.g. every variety over a finite field has $I(V) = 1$ (cf. Lemma 11); nevertheless computing $\mathcal{S}(V)$ is still a nontrivial task.

¹Note that this holds – vacuously – even when $g = 1$.

It is natural to ask:

Question 1. *Fix a field K . For which pairs $(g, I) \in \mathbb{N} \times \mathbb{Z}^+$ does there exist a curve $C_{/K}$ with $I(C) = I$?*

As above, the existence of the canonical divisor implies that a necessary condition is $I \mid 2g - 2$. This condition is, of course, not sufficient: e.g., we have $I(C) = 1$ for all curves when K is finite or PAC,² whereas if K is \mathbb{R} (or is real-closed, or pseudo-real closed) we have $I(C) \mid 2$.

In contemporary arithmetic geometry, the fields of most interest are those which are infinite and finitely generated (“IFG”).

Conjecture 2. *Let K be an IFG field. Then for any g and I with $I \mid 2g - 2$, there exists a curve $C_{/K}$ of genus g with $I(C) = I$.*

Remark 1.1: It is easy to see that Conjecture 2 holds for $g = 0$.

Remark 1.2: The main result of [3] is that Conjecture 2 holds for $g = 1$ when K is a number field. Indeed, in genus one it is tempting to make a much stronger conjecture: see [6, Conjecture 1].

Let us now present evidence for Conjecture 2 for curves of higher genus ($g \geq 2$). The following result uses the author’s work on the genus one case together with some simple covering considerations (essentially those suggested to the author by Bjorn Poonen in 2003) to attain a solution for “small indices.”

Theorem 3. *Let K be a number field, $g \in \mathbb{N}$ and $k \in \mathbb{Z}^+$ with $k \mid g - 1$. Then there exists a curve $Y_{/K}$ of genus g and index $I = \frac{g-1}{k}$.*

Proof. Since K has characteristic different from 2, it is especially easy to see that there exist (hyperelliptic) curves over K of all genera with K -rational (Weierstrass) points; we may therefore assume that $I > 1$. By Remark 1.2 there exists a curve $X_{/K}$ of genus one and index I . By [5, Prop. 13], there exist linearly equivalent K -rational divisors D_1 and D_2 on C , both effective of degree kI , such that the support of $D_1 - D_2$ has cardinality $2kI$. Let $f \in K(X)$ be a rational function with divisor $D_1 - D_2$, and let $\varphi : Y \rightarrow X$ be the branched covering corresponding to the extension of function fields $K(X)(\sqrt{f})/K(X)$. By the Riemann-Hurwitz formula, Y has genus $g = kI + 1$. We have $I(Y) \leq I(X)$ (a special case of Lemma 10, below). Conversely, any point P in the support of D_1 has degree I and is a ramification point for φ , so its unique preimage $\tilde{P} \in Y(\overline{K})$ has degree I . Thus we have $I(Y) = m(Y) = I$. \square

We shall present a technique for constructing curves C over local fields with very detailed information on the set $\mathcal{S}(C)$ of finite degree splitting fields. In some cases – e.g., if k is finite – our information is complete. Here is our main result:

²A field K is **P**seudo **A**lgebraically **C**losed if every variety $V_{/K}$ has a rational point. This includes separably closed fields, but there are many others: see [9].

Main Theorem. *Let K be discretely valued Henselian, with perfect residue field k . Assume that there is a cyclic, degree I , unramified extension K_I/K . For $g \in \mathbb{N}$ such that $I \mid 2g - 2$, there exists a curve $C_{/K}$ with the following properties:*

- a) *If $L \supset K_I$, then L splits C .*
- b) *If L splits C and L does not contain K_I , then: $g \neq 1$, I is even, $2 \mid e(L/K)$ and $L \supset K_{I/2}$, the unique subextension of K_I/K of degree $\frac{I}{2}$.*
- c) *Suppose that $\text{Br}(l)[2] = 0$ for all finite extensions l/k . Then the converse of b) holds: if $g \neq 1$, I is even, $2 \mid e(L/K)$ and $L \supset K_{I/2}$, then L splits C .*

Remark 1.3: It follows from parts a) and b) that the curve $C_{/K}$ has index I . So all possible indices $I \mid 2g - 2$ arise for curves of genus g provided that there exist cyclic unramified extensions of all degrees. In particular this holds when the residue field is *finitely generated*, when we may construct K_I by adjoining suitable roots of unity.

Remark 1.4: Some hypothesis on the existence of unramified extensions is necessary, since if k is algebraically closed, then $I(C) \mid g - 1$ [2, Remark 1.8]. On the other hand, one could ask for a classification of all possible indices under the milder assumption that K admits an unramified quadratic extension, e.g. in the case $K = \mathbb{R}((T))$. This seems interesting, but we shall not pursue it here.

Corollary 4. *Let K be an infinite, finitely generated field. For any $g \in \mathbb{N}$, there exists a finite extension L/K and a genus g curve $C_{/L}$ with $I(C) = 2g - 2$.*

Proof. K admits a discrete valuation v with finitely generated residue field k , so by Remark 1.3 we may apply our Main Theorem to the Henselization K_v of K . We thus get a curve C of genus g and index I defined over K_v , which is an algebraic extension of K ; it is evidently defined over some finite extension L of K . \square

Remark 1.5: Only a few days after the results of this paper were first obtained, I received a copy of the 2006 Berkeley thesis of S.I. Sharif [15], which contains closely related results.

Theorem 5. (*Sharif, [15]*)

- a) *Let K be a locally compact discretely valued field of characteristic different from 2. Then for any $(g, I) \in \mathbb{N} \times \mathbb{Z}^+$ with $I \mid 2g - 2$, there exists a curve $C_{/K}$ of genus g and index I .*
- b) *For any $g \in \mathbb{N}$ and $I \in \mathbb{Z}^+$ such that $4 \nmid I \mid 2g - 2$, there exists a number field $K = K(g, I)$ and a curve $C_{/K}$ of genus g and index I .*

By Remark 1.3, part a) of Theorem 5 is a special case of our Main Theorem, whereas part b) is similar in spirit to Theorem 3 and Corollary 4 but not directly comparable to either one. On the other hand, Sharif's results go further than those presented here in that he also considers the possible values of the *period* P (the least positive degree of a K -rational divisor class), and – comparing with the restrictions on period and index obtained by Lichtenbaum – his constructions give the complete list of possible values of (g, P, I) for curves over locally compact fields of characteristic different from 2.

The strategy of Sharif's proof – construction of degree two covers of curves of genus one and two via p -adic theta functions – is quite different from ours.

The proof of the Main Theorem proceeds in three steps. The first step is to invoke

a fundamental result in deformation theory: given a semistable curve $C_{/k}$ defined over the residue field, there is a regular arithmetic surface over the valuation ring with smooth generic fiber and special fiber isomorphic to $C_{/k}$.

Next we attempt to compute the set $\mathcal{S}(C)$ of finite splitting fields solely in terms of the special fiber $C_{/k}$. If we assume an additional geometric ‘‘Hypothesis (A)’’ as well as the algebraic ‘‘Hypothesis (B)’’ that for all finite extensions l/k , every genus zero curve over l has an l -rational point, then we can in fact give such a description: Theorem 8a). The information lost in not assuming (B) leads exactly to the necessary but generally not sufficient condition of part b) of the Main Theorem. However, without assuming either (A) or (B) one can still compute the index $I(C)$ in terms the special fiber. Indeed, the notion of index can be extended to certain singular schemes in such a way that the index does not change upon passage from the generic fiber to the special fiber of a semistable arithmetic surface, an *Index Specialization Theorem* (Theorem 9). This should be compared with earlier work that computes the index of an arbitrary curve over a local field with finite residue field in terms of the special fiber of its minimal regular model [8], [2], [13, §9.2].

Combining the first two steps, it suffices to construct semistable curves over k with prescribed dual graph and Galois action. A theorem of Pál asserts that there are essentially no restrictions on realizing a finite graph as the dual graph of a semistable curve, compatibly with the Galois action. Thus the problem is reduced to constructing connected finite graphs of prescribed Euler characteristic and endowed with an automorphism of order I with certain fixed-point properties. As it turns out, this problem is solved by a well-known family of graphs, the *Möbius ladders*.

In §2 we present background information on semistable arithmetic surfaces and then embark on a systematic attempt to recover $\mathcal{S}(C)$ or at least $I(C)$ from the special fiber, proving Theorems 8 and 9. Fair warning: we wrestle with this problem more extensively than is necessary to prove the Main Theorem. (The reader who is looking for the quickest possible route to the Main Theorem, especially in the case of finite residue field, may skip §2.3 and §2.5, which are of a more technical nature than the rest of the paper.) In §3 we flesh out the above sketch and then solve the graph-theoretical problem, completing the proof of the Main Theorem.

In §4 we discuss possible generalizations of Theorem 6.

2. LOCAL POINTS ON SEMISTABLE ARITHMETIC SURFACES

The following notation will be in force for the remainder of the paper: K is a Henselian discretely valued field with valuation ring R and perfect residue field k . Moreover C is a curve over K with semistable reduction – that is, C may be realized as the generic fiber of an arithmetic surface $C_{/R}$ whose special fiber is a semistable curve $C_{/k}$.

As this terminology is widely used but not completely standardized, we give careful definitions – ones which are most convenient for our purposes – in §2.1 and §2.2. But let us now disclose the key point. On the one hand, our Diophantine application requires us (via Hensel’s Lemma) to work with regular arithmetic surfaces. Nevertheless we must also consider non-regular arithmetic surfaces, because a regular arithmetic surface with semistable, but singular, special fiber becomes non-regular upon making a ramified base change. A regular model can then be

obtained by repeatedly blowing up, a process which is very well understood in the geometric setting (i.e., when $k = \bar{k}$) but which in the general case carries some unexpected (to the author, at least) subtleties, as discussed in §2.2 and §2.3.

The recent work [?] is an excellent reference for the background material of the next two subsections, notwithstanding some minor variations in terminology.

2.1. Semistable curves.

Definition: A *semistable curve* is a one-dimensional projective k -scheme which is geometrically connected, geometrically reduced and whose only singularities are ordinary double points.

Remark 2.1.1: Being a semistable curve is a geometric notion: if C is a k -scheme and l/k is any field extension, then C is a semistable curve iff C_l is a semistable curve over l .

Consider the decomposition $C_{/\bar{k}} = \sum_{i=1}^N C_i$ of $C_{/\bar{k}}$ into nonempty, irreducible closed subsets, which we call the *components* of C .

There is a natural \mathfrak{g}_k -action on the set of components. A component C_i is *defined* over a finite field extension l/k if $\mathfrak{g}_l = \text{Gal}(\bar{l}/l)$ fixes C_i . There is evidently a unique minimal such field extension (necessarily Galois over k), which we denote by l_i . Let $d_i = [l_i : k]$, and put

$$C_i^o := (C_i)_{/l_i} \cap C^{ns},$$

i.e., the locus of points on the i th component which are not nodal points on C .

Let l/k be a finite extension and $q \in C(l)$ be a nodal point. Consider the preimage $\pi^{-1}(q)$ of q under the normalization map $\tilde{C} \rightarrow C$. We say that q is *l -split* if $\pi^{-1}(q)$ consists of two l -rational points. Otherwise $\pi^{-1}(q)$ consists of a pair of points conjugate over a quadratic extension m/l , and in this case we say q is *non-split* and m/l is the splitting field.

It will be convenient to introduce the (so-called) dual graph $\mathcal{G} = \mathcal{G}(C_{/k})$, an undirected, connected, finite graph whose vertices are the components of C , and where vertices C_i and C_j are linked by $C_i \cdot C_j$ edges. The natural action of the Galois group \mathfrak{g}_k on components and on singular geometric points gives rise to an action of \mathfrak{g}_k on \mathcal{G} by graph-theoretical automorphisms.

Example 2.1.2: Let k a field of characteristic different from 2. The equation $x^2 + y^2 = 0$ defines a semistable curve C in \mathbb{P}^2 . If -1 is a square in k , then C is rationally isomorphic to two copies of the projective line intersecting at a single k -rational point. Otherwise this same description holds over $k(\sqrt{-1})$, but over k the two components are permuted by the Galois group of $k(\sqrt{-1})/k$, and the intersection point $(0, 0, 1)$ is singular, defined over k , and is the only k -rational point on C . In each case the dual graph has two vertices connected by a single edge. In the first case the Galois action on the dual graph is trivial; in the second case it interchanges the two vertices and “flips” the unique edge.

Generalizing this example, we say what it means for an edge E in the dual graph of C to be a *stable inversion*. If E runs between distinct vertices corresponding to components $C_i \neq C_j$, then by definition this means that the pair $\{C_i, C_j\}$ is \mathfrak{g}_k -stable but there exists $\sigma \in \mathfrak{g}_k$ such that $\sigma(C_i) = C_j$. If E is a loop corresponding to a nodal point on a single component C_i , then E is a stable inversion if C_i is \mathfrak{g}_k -stable and the corresponding nodal point is a nonsplit k -rational singular point.³

2.2. Arithmetic surfaces. An *arithmetic surface* C/R is an R -scheme which is flat, projective, excellent, normal, integral, of relative dimension one, and whose generic fiber is a(n as ever smooth, projective, geometrically integral) curve over K . We call an arithmetic surface *semistable* if its special fiber is a semistable curve.⁴

The structure of the special fiber of a regular arithmetic surface with generic fiber C/K is closely related to the existence of rational points on C .

Proposition 6. (*Hensel's Lemma*) *For a regular arithmetic surface C/R , the following are equivalent:*

- a) $C(K) \neq \emptyset$.
- b) C/k has a nonsingular k -rational point.

Proof. E.g., [11, Lemma 1.1]. □

Now let C be an arithmetic surface over R , and let L/K be a finite field extension, with valuation ring S . Then $C \otimes_R S$ is an arithmetic surface over S whose generic fiber is C/L . However, $C \otimes_R S$ is not necessarily regular, even if C is regular. By dévissage, it suffices to consider the unramified and totally ramified cases.

Suppose first that L/K is unramified. Then $C \otimes_R S$ is regular iff C is regular. Combining with Hensel's Lemma, we conclude that C has a rational point in an unramified extension L/K iff the special fiber C/k has a nonsingular l -rational point, where l/k is the corresponding residual extension.

Now consider the effect of making a totally ramified base extension L/K of degree $e > 1$. Then $C \otimes_R S$ is regular iff C is smooth over R . The sufficiency is clear, so conversely suppose that there is a singular point $q \in C(\bar{k})$. Then the completed local ring of q in $C \otimes_R R^{\text{unr}}$ is isomorphic to $R^{\text{unr}}[[x, y]]/((xy - \pi^{\ell(q)}))$, where R^{unr} is the valuation ring of the maximal unramified extension of K , π is a uniformizing element for R , and the positive integer $\ell(q)$ is a local invariant of the singularity, its *length*. This local ring is regular iff $\ell(q) \leq 1$. Evidently the effect of basechanging from R^{unr} to the totally ramified extension S^{unr} on this complete local ring is to multiply its length by e .

To obtain from $C \otimes_R S$ a regular model of the generic fiber C/L , it suffices to perform $\ell(q) - 1$ blowups on each singular point q , introducing a chain of $\ell(q) - 1$ rational curves. Note that the effect on the dual graph is just that of (possibly non-uniform) ‘‘barycentric’’ subdivision: on each edge $E(q)$ we introduce $\ell(q) - 1$ additional vertices.

This, however, is merely a geometric description: to work over R and S rather than R^{unr} and S^{unr} requires some further care. First, rather than thinking of performing the blowup on singular points of the geometric fiber, we blow up the closed

³The two cases can be consolidated by thinking about the Galois action on tangent directions at the nodal point.

⁴It would be more pedantically correct to say that it has semistable reduction, but the elision is quite common: c.f. ‘‘semistable elliptic curve.’’

point q (which may be identified with the \mathfrak{g}_k -orbit of a given geometric singular point); this determines a k -model for the geometric special fiber. The Galois action on the “exceptional vertices” of the dual graph – i.e., those coming from the exceptional components – is the one induced by subdivision. The only slight subtlety is that if an automorphism $\sigma \in \mathfrak{g}_k$ inverts an edge $E(q)$ (by switching its initial and terminal vertices), then σ carries the i th exceptional component to the $(\ell(q) - i)$ th exceptional component. In particular, an exceptional component is \mathfrak{g}_k -stable iff either both components at the extremities of the chain are \mathfrak{g}_k -stable, or if it is the $(\frac{\ell(q)}{2})$ th component in a chain corresponding to an edge $E(q)$ of even length $\ell(q)$ which is stably inverted by Galois.

Remark 2.2.1: Similarly, if a component C_i has an l -rational nonsplit self-intersection point q , then an automorphism $\sigma \in \mathfrak{g}_l$ inducing the nontrivial automorphism on the Galois group of the splitting field m/l will interchange the i th and $(\ell(q) - i)$ th exceptional components on a blowup.

Finally, if we have, as above, a Galois-stable exceptional component E on the special fiber of our regular model of C/L , then E defines a smooth, projective genus 0 curve over k . We would like to know whether E is k -rationally isomorphic to the projective line. Recalling that a genus 0 curve other than \mathbb{P}^1 defines a nontrivial element in $\text{Br}(k)[2]$, we certainly have $E \cong_k \mathbb{P}^1$ if $\text{Br}(k)[2] = 0$. This also holds if the singular point q is k -split, for then each of the components C_i and C_j whose intersection is q is \mathfrak{g}_k -stable, and it follows that all the intersection points of the exceptional components lying over q are k -rational (and a genus 0 curve with a k -rational point is isomorphic to the projective line).

In general, a \mathfrak{g}_k -stable exceptional component need not be k -isomorphic to the projective line, a phenomenon which is responsible for the somewhat complicated statement of the Main Theorem. We study this further in the next section.

2.3. **The case of genus 0.** Let C/K be a curve of genus 0. Let us assume for now that K does not have characteristic 2, so that C has a defining equation of the form

$$C : aX^2 + bY^2 = cZ^2$$

with $a, b, c \in K^\times$, and after rescaling, reordering and adjusting coefficients by squares, we may assume that $a, b, c \in R$ and $a, b \in R^\times$. Then the equation defines a regular arithmetic surface over R . There are three possibilities for the special fiber:

(i) If $c \in R^\times$, then the special fiber defines a smooth conic over k . In this case, C is split by an extension L/K iff it is split by the maximal unramified extension L'/K .

(ii) If $c \in R \setminus R^\times$, then the special fiber has equation $X^2 + \frac{b}{a}Y^2 = 0$, so has two geometric components C_1, C_2 , each smooth of genus 0, and intersecting at a k -rational point.

(iia) If $\frac{-b}{a} \in k^{\times 2}$, the singularity is split, the \mathfrak{g}_k -action on the components is trivial, and $C_1 \cong C_2 \cong \mathbb{P}^1$ so that by Hensel's Lemma C has K -rational points.

(iib) If $\frac{-b}{a}$ is not a square in k then the singularity is nonsplit and $C^{\text{ns}}(k) =$

$C(K) = \emptyset$. Suppose L/K is a totally ramified extension, of degree e . From the previous discussion L can only split C if e is even, in which case a regular model C'_S is obtained by blowing up the singular point $e - 1$ times and the middle exceptional component is stable under $\text{Gal}(k(\sqrt{\frac{-b}{a}})/k)$ and hence gives a smooth conic curve $E_{/k}$ which is determined up to isomorphism by its class, say $[E]_L$, in $\text{Br}(k)[2]$.

We can identify this class in terms of Galois cohomology, as follows: recall from [14, Theorem 2, § XII.3] the short exact sequence

$$(1) \quad 0 \rightarrow \text{Br}(k) \xrightarrow{\iota} \text{Br}(K) \xrightarrow{\tau} \text{Hom}(\mathfrak{g}_k, \mathbb{Q}/\mathbb{Z}) \rightarrow 0.$$

Moreover, by [14, Exercise 2, § XII.3] this exact sequence is functorial in K : in the case of a totally ramified extension L/K of degree e we get a map from the short exact sequence to

$$0 \rightarrow \text{Br}(k) \xrightarrow{\iota} \text{Br}(L) \xrightarrow{\tau} \text{Hom}(\mathfrak{g}_k, \mathbb{Q}/\mathbb{Z}) \rightarrow 0,$$

in which the induced endomorphism on $\text{Br}(k)$ is the identity and that on $\text{Hom}(\mathfrak{g}_k, \mathbb{Q}/\mathbb{Z})$ is multiplication by e . Therefore, given any element η of $\text{Br}(K)[2]$ and a totally ramified extension L/K of even degree e , the restriction $\eta|_L$ of η to $\text{Br}(L)$ lies in $\text{Br}(k)$. Our genus zero curve $C_{/K}$ gives rise to a class $[C] \in \text{Br}(K)[2]$, and we have:

Proposition 7. *For any totally ramified extension L/K of even degree,*

$$[C]|_L = [E]_L.$$

Proof. As noted above, the restriction of $[C]$ to L is unramified, so is the image under ι of the Brauer class of a conic E' defined over k . We wish to show that $E \cong E'$, and for this it suffices to show that a (possibly transcendental) field extension l/k splits E iff l splits E' : indeed, if this holds we may take successively $l = k(E)$ and $l = k(E')$ and apply Witt's theorem: $\text{Br}(k(E)/k) = \{1, [E]\}$ [17]. But this fact follows almost tautologically from the setup: we may extend S to a Henselian discrete valuation ring S_l with quotient field L_l , residue field l , and such that a uniformizer for S remains a uniformizer for S_l . Then $C' \otimes_S S_l$ is a regular arithmetic surface, and we have that

$$E(l) \neq \emptyset \iff C(L_l) \neq \emptyset \iff E'(l) \neq \emptyset.$$

□

Example 2.3.1: Suppose $\text{Br}(k)[2] = 0$, e.g. k is finite, PAC, or of characteristic 2 (recall that k is assumed perfect). Let $C_{/K}$ be a genus zero curve without rational points. Then we are necessarily in Case (iib). Moreover, there exists a unique unramified quadratic splitting field L/K for C (the splitting field of the singular point) and a totally ramified extension splits C iff it has even degree. This can be seen either from our geometric considerations or by using the functorial properties of (1); note that the latter is also valid when $\text{char}(K) = 2$.

Example 2.3.2: Consider the regular arithmetic surface over $\mathbb{R}[[t]]$ with equation

$$C : X^2 + Y^2 = tZ^2,$$

whose special fiber ($t = 0$) is the semistable curve of Example 2.1.1, nonsplit since -1 is not a square in \mathbb{R}^\times . The curve C is split by $\mathbb{R}((\sqrt{t}))$ but not by $\mathbb{R}((\sqrt{-t}))$.

This means that blowing up the singular point on $C \otimes_{\mathbb{R}[[t]]} \mathbb{R}[[\sqrt{-t}]]$ yields an exceptional component which is not \mathbb{R} -isomorphic to the projective line. Moreover, using (1), $\text{Br}(\mathbb{R}((t))) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the other two nontrivial elements are represented by the conjugate conic $X^2 + Y^2 = -tZ^2$ (Case (iib) again) and the isotrivial conic $X^2 + Y^2 = -Z^2$ (Case (i)). Since $X^2 + Y^2 = \pm tZ^2$ have the same special fiber, we see that the k -rational structure of an exceptional divisor obtained by blowing up a nonsplit singular point depends upon the arithmetic surface and not only on its special fiber. Moreover, in this case there is no genus 0 curve without K -rational points that is split by every ramified quadratic extension.

It would be interesting to explore this phenomenon in higher genus and to see to what extent it is controlled by the existence of maps from $C_{/K}$ to a conic curve.

2.4. A computation of $\mathcal{S}(C)$. Next we shall show that for a certain subclass of semistable arithmetic surfaces $C_{/R}$ we can give a complete and concrete description of the set $\mathcal{S}(C)$ of splitting fields of the generic fiber in terms of data of the special fiber. Consider the following additional hypotheses:

(A) For every finite extension l/k , every component C_i which is defined over l has an l -rational point which is not a nodal point of C .

(B) $\text{Br}(l)[2] = 0$ for every finite extension l/k .

Theorem 8. *Let $C_{/R}$ be a regular, semistable arithmetic surface.*

a) Assume hypotheses (A) and (B). Then a finite extension L/K splits C if and only if at least one of the following occurs:

Case 1: *The residual extension l/k contains l_i for some i , or:*

Case 2: *l/k does not contain any l_i , the ramification index $e(L/K)$ is even, and $\mathfrak{g}_l = \text{Gal}(\bar{l}/l)$ stabilizes a pair of intersecting components.*

*b) If we assume only hypothesis (A), then the conclusion of part a) holds, except that the conditions of **Case 2** are necessary, but not generally sufficient, for $C(L) \neq \emptyset$.*

Proof. Let L'/K be the maximal unramified subextension of L/K . By Hensel's Lemma, $C(L') \neq \emptyset$ iff C has a nonsingular l -rational point. This can only happen if there exists a \mathfrak{g}_l -stable component C_i – i.e., if $l \supset l_i$ for some i – and (A) ensures that this necessary condition is also sufficient.

It remains to decide when $C(L') = \emptyset$ but $C(L) \neq \emptyset$. From the discussion in §2.2 this happens iff $e(L/L')$ is even, \mathfrak{g}_l acts on the dual graph by a stable inversion of distinct components (since if a component C_i had an l -rational self-intersection point, by (A) it would also have an l -rational point which is nonsingular on the special fiber) and the middle exceptional component E is k -rationally isomorphic to the projective line. Since (B) ensures that $E \cong_k \mathbb{P}^1$, this completes the proof. \square

Notice that even without (B) we know the degree of any possible splitting field, so in particular we can compute the index of C . In fact we can perform the index computation even without (A), which brings us to the next result.

2.5. The index specialization theorem. For a reduced, finite-type scheme $S_{/k}$, define its *nonsingular index* $I^{\text{ns}}(S)$ to be the least positive degree of a k -rational zero cycle on the nonsingular locus S^{ns} . Put $I_i := I^{\text{ns}}((C_i)_{/l_i})$.

Theorem 9. *Let $C_{/R}$ be a regular arithmetic surface with generic fiber $C_{/K}$ and semistable special fiber $C_{/k}$. Then*

$$I(C_{/K}) = I^{\text{ns}}(C_{/k}) = \gcd_i(d_i \cdot I_i).$$

A conjectural strengthening of this theorem will be made in §4.

Lemma 10. *If $V_{/k}$ is a finite-type reduced scheme and l/k is a finite field extension, then $I^{\text{ns}}(V_{/k}) \mid [l : k] \cdot I^{\text{ns}}(V_{/l})$.*

Proof. Let D_l be an l -rational zero-cycle on V^{ns} of degree $I(V_{/l})$; its trace from l down to k is a k -rational zero-cycle of degree $[l : k] \cdot I(V_{/l})$. \square

Lemma 11. *Let V and W be reduced, finite-type nonsingular k -schemes. If there exists a k -morphism $\varphi : V^{\text{ns}} \rightarrow W^{\text{ns}}$, then $I^{\text{ns}}(W) \mid I^{\text{ns}}(V)$.*

Proof. Degree N zero-cycles on V^{ns} are mapped to degree N zero-cycles on W^{ns} . \square

Lemma 12. *Let W be a complete, geometrically integral k -variety assumed to admit a resolution of singularities. Then for any nonempty Zariski open-subset U of W , we have $I^{\text{ns}}(U) = I^{\text{ns}}(W)$.*

Proof. If $k \cong \mathbb{F}_q$ is finite, then much more is true: for all finite-type geometrically integral schemes $W_{/\mathbb{F}_q}$ $I^{\text{ns}}(W) = 1$. This holds, e.g., because the Weil bounds for curves over finite fields imply that any infinite algebraic extension of a finite field is PAC [9, Cor. 11.2.4] and thus W has points rational both over an extension of the form $\mathbb{F}_{q^{2^a}}$ and over an extension of the form $\mathbb{F}_{q^{3^b}}$.

When k is infinite, let $\pi : \tilde{W} \rightarrow W$ be a resolution of singularities of W , $V = W^{\text{ns}}$ be the nonsingular locus, and let $U \subset V$ be a nonempty Zariski-open subset. Also put $\tilde{V} = \pi^{-1}(V)$ and $\tilde{U} = \pi^{-1}(U)$; by definition of resolution of singularities, π restricted to \tilde{V} (resp. to \tilde{U}) induces an isomorphism onto V (resp. onto U). So let Z be a k -rational zero cycle on W which is supported on V , and \tilde{Z} its preimage on \tilde{V} . The point of this construction is that we have reduced to a fact about Chow groups of complete, nonsingular varieties, on which rationally equivalent zero-cycles have the same degree. Applying a known moving lemma [7, §3, Complément], we can find a rationally equivalent zero-cycle \tilde{Z}' supported on \tilde{U} , and then $Z' := \pi(\tilde{Z}')$ is a divisor on W , supported on U , with $\deg(Z') = \deg(Z)$. \square

Corollary 13. *Let $C_{/k}$ be a geometrically reduced (but possibly incomplete and/or singular) curve. Then the nonsingular index $I^{\text{ns}}(C)$ is unchanged by the removal of finitely many closed points.*

Proof. Let C^0 be the complement in C of a finite set of closed points. Embed C in some projective space and let \overline{C} be its projective closure. As is well-known, in the one-dimensional case normalization provides a resolution of singularities of \overline{C} . So Lemma 12 applied to \overline{C} shows

$$I^{\text{ns}}(C^0) = I^{\text{ns}}(\overline{C}) = I^{\text{ns}}(C).$$

\square

We are now ready to prove Theorem 9.

Proof. Step 1: We will show that $I^{\text{ns}}(C/k) = \gcd_i d_i I_i$. By applying Corollary 13 to $(C_i)_{/l_i}$ we get

$$(2) \quad I_i = I^{\text{ns}}((C_i)_{/l_i}) = I^{\text{ns}}(C_i^0) = I(C_i^0).$$

Next we claim that for any i , $1 \leq i \leq N$, we have:

$$I^{\text{ns}}(C/k) = I(C_{/k}^{\text{ns}}) \mid d_i I(C_{/l_i}^{\text{ns}}) \mid d_i \cdot I(C_i^0) = d_i \cdot I_i.$$

Indeed, we get the first divisibility by applying Lemma 10 to C^{ns} and l_i/k , the second divisibility by applying Lemma 11 to $C_i^0 \rightarrow (C^{\text{ns}})_{/l_i}$, and the equality by (2). Hence

$$I^{\text{ns}}(C/k) \mid \gcd d_i I_i.$$

For the converse, $I^{\text{ns}}(C/k)$ is the gcd of all degrees of field extensions l/k such that C has a smooth l -rational point P . Thus l must be a field of definition for the component on which P lies – i.e., $l_i \subset l$, and then clearly $I_i \mid [l : l_i]$.

Step 2: It follows from Hensel's Lemma that $I(C/K) \mid I^{\text{ns}}(C/k)$. More precisely, the fields l for which C acquires a smooth l -rational point correspond to the unramified splitting fields. For the converse, let L/K be any splitting field of C ; we will show that $I^{\text{ns}}(C/k) \mid [L : K]$.

Let L'/K be the maximal unramified subextension of L/K ; denote the residual extension by l/k . If $L' = L$ there is nothing to show. So we may assume that $[L : L'] = e(L/K) > 1$, and that there is an l -rational nodal point q on C .

Consider first the case in which q is the intersection of distinct components C_i, C_j . Since q is l -rational, $S = \{C_i, C_j\}$ is \mathfrak{g}_l -stable. If the singularity is split – i.e., each of C_i, C_j are \mathfrak{g}_l -stable – then q is a nonsingular l -rational point on the geometrically integral curve C_i , so $I^{\text{ns}}((C_i)_{/l}) = 1$. By (2), $I^{\text{ns}}(C_{/l}) = 1$, so by Lemma 10

$$I^{\text{ns}}(C/k) \mid [l : k] = [L' : K] \mid [L : K].$$

Otherwise we are in the nonsplit case, in which the \mathfrak{g}_l -action on S cuts out a quadratic extension m/l , and as usual, to get a $\text{Gal}(m/l)$ -stable exceptional component we need $2 \mid e(L/K) = [L : L']$. Moreover, q is an m -rational nonsingular point on the geometrically integral curve C_i . Taking M/K to be the corresponding unramified extension and again applying Lemma 10, we get

$$I^{\text{ns}}(C/k) \mid [m : k] = 2 \cdot [L' : K] \mid [L : K].$$

The case in which q is a self-intersection point on C_i is similar. Suppose first that the singularity is split: then the preimages are l -rational on the normalization \tilde{C}_i , so that $I^{\text{ns}}(C_i) = 1$ and we deduce $I^{\text{ns}}(C/k) \mid [L' : K]$ as above. Finally, if the singularity is nonsplit, then by Remark 2.2.1 we once again need $2 \mid [L : L']$ to get a $\text{Gal}(m/l)$ -stable exceptional component, and then we get $I^{\text{ns}}(C/k) \mid [L : K]$. \square

3. PROOF OF THE MAIN THEOREM

We will construct semistable arithmetic surfaces satisfying (A) of §2.4, so that – modulo complications arising from failure of exceptional components to have points rational on the ground field if (B) is not assumed – the set of splitting fields is entirely determined by the Galois action on the dual graph. In fact, we will place ourselves in a situation in which we need only construct the dual graph and not the arithmetic surface itself. This is done via the following two results:

Theorem 14. (Conrad) *For any semistable curve $C_{/k}$, there is a regular arithmetic surface whose special fiber is isomorphic to C and whose generic fiber is a curve over K .*

Proof. This is Theorem B.2 of [1, Appendix]. □

Thus it suffices to construct suitable semistable curves over the residue field k . We will in fact construct *totally degenerate* semistable curves, namely with each component of geometric genus 0. For this:

Lemma 15. *Let \mathcal{G} be any connected graph in which each vertex has degree at most 3. Let G be a finite group acting on \mathcal{G} by automorphisms. Given a field k , a Galois extension l/k and an isomorphism from $\mathfrak{g}_{l/k}$ to G , there is a totally degenerate semistable curve $C_{/k}$ whose dual graph is isomorphic to \mathcal{G} , under an isomorphism which identifies the Galois action on \mathcal{G} with the action of G .*

Proof. This is shown in [12] under the hypothesis that k is infinite but without the hypothesis that the vertex degrees of \mathcal{G} are at most 3. The infinitude of k is used precisely to ensure that the intersection points of the graph can be taken to be k -rational points of \mathbb{P}^1_k . Since $\#\mathbb{P}^1(k) \geq 3$ for all k , the argument goes through verbatim with the hypothesis of degree at most 3. □

Recall that the arithmetic genus of a totally degenerate semistable curve C_k (which is the genus of any generically smooth lift $C_{/K}$ in the usual sense) is just $1 - \chi(\mathcal{G})$, where χ is the Euler characteristic of the dual graph in the usual topological sense, computable as the number of vertices minus the number of edges.

The curves constructed by Lemma 15 satisfy hypothesis (A) unless the residue field k is \mathbb{F}_2 . More precisely, what we need is that for each finite extension l/k , every component which is defined over l has at most $\#l$ singular points. Since our graphs have degree at most 3, the only problematic case is when $k = \mathbb{F}_2$ and $I = 1$ (because if $I > 1$, we only want points over an extension with larger residue field). But this is a trivial case: it is enough, for instance, to find a nonsingular curve $C_{/\mathbb{F}_2}$, of genus g , and with $C(\mathbb{F}_2) \neq \emptyset$. Or, staying with the same graph-theoretical strategy, we need only to find, for all $g \geq 0$, a connected graph with Euler characteristic $1 - g$, in which each vertex has degree at most 3, and at least one vertex has degree at most 2. Of course such graphs exist: for $g = 0$ take the graph with one vertex and no edges (the dual graph of \mathbb{P}^1), and for $g \geq 1$ we can build such a graph out of g ‘‘coathangers’’ (the graph with vertex set $\{0, 1, 2, 3\}$ and $0 \sim 1, 0 \sim 2, 0 \sim 3, 2 \sim 3$). Henceforth we will assume that $I > 1$.

Let G be a group and $S \subset G$ such that $S = S^{-1}$, $1 \notin S$, and $\langle S \rangle = G$. We define the Cayley graph $\text{Cay}(G, S)$, a simple (no loops, no multiple edges) undirected graph whose vertex set is G itself, and with

$$g \sim g' \iff \exists s \in S \mid gs = g'.$$

Note the following (almost tautological) properties of $\text{Cay}(G, S)$: (i) it is connected; each vertex has degree $\#S$; (ii) it admits a left G -action which is free on vertices, and free on edges unless S contains an element of order 2.

(iii) If G is finite,

$$\chi(\text{Cay}(G, S)) = \#G \left(1 - \frac{\#S}{2}\right).$$

(iv) If $\rho : H \hookrightarrow G$ is an embedding, then H acts on $\text{Cay}(G, S)$, freely on vertices and freely on edges unless $\rho(H) \cap S$ contains an element of order 2.

Now let $G_I = \langle \sigma \mid \sigma^I = 1 \rangle$, and identify G_I with $\mathfrak{g}_{K_I/K} = \mathfrak{g}_{k_I/k}$.

When $g = 0$ and $I = 2$, we can take $\mathcal{G} = \text{Cay}(G_2, \{\sigma\})$, the unique connected graph with two vertices and one edge: $\chi = 1$. Since the generator has order 2, the unoriented edge gets stabilized, so by Theorem 8 we get the ‘‘Case 2’’ splitting behavior indicated in the theorem.

When $g = 1$ and $I > 2$, we take $\mathcal{G} = \text{Cay}(G_I, \{\sigma, \sigma^{-1}\})$, the I -cycle: $\chi = 0$. Here G acts freely on the edges, so – cf. Remark 2.1 – we get the ‘‘Case 1’’ splitting behavior indicated in the theorem.

When $g = 1$ and $I = 2$ we can take \mathcal{G} to be the 2-cycle, and let G_I act by ‘‘180 degree rotation’’, i.e., by swapping both vertices and both edges: $\chi = 0$, Case 1. This graph is nonsimple and *a fortiori* not a Cayley graph according to our setup. If we insist on seeing a Cayley graph construction, fix $N > 1$ and let $\rho : G_2 \hookrightarrow G_{2N}$ be the embedding $\sigma \mapsto \sigma^N$.

When $g > 1$ and $I = 2g - 2$, take $\mathcal{G} = \text{Cay}(G_I, \{\sigma, \sigma^{-1}, \sigma^{g-1}\})$. Or, in plainer terms, start with the $2g - 2$ cycle and connect each pair of antipodal points by an edge: these ‘‘spokes’’ do not ruin the obvious G_{2g-2} action by rotations.

This second description is graph-theoretically correct (which is, of course, all that matters for us) but geometrically wrong: the graph does not really live in the Euclidean plane because the spokes would have to meet at the center of the circle, adding an unwanted (and G_I -fixed) vertex. Indeed, when $g = 4$ the graph is precisely the complete bipartite graph $K_{3,3}$, and for larger g the graph contains $K_{3,3}$ as a topological subgraph, so these graphs are *not* embeddable in the Euclidean plane!⁵ So here is a ‘‘better’’ geometric description: take a rectangle of length g and height 1, subdivide the top and bottom sides into $g - 1$ equal parts, and draw in the $g + 1$ equidistant vertical lines linking each vertex on the top to its corresponding bottom vertex. The resulting graph has $2g$ vertices and $g + 2(g - 1)$ edges. Now identify the right and left sides of the rectangle with a half-twist, getting a graph embedded isometrically into the Möbius band with $2g - 2$ vertices and $g + 2(g - 1) - 1 = 3g - 3$ edges with a natural action of the cyclic group G_I by unit length horizontal rotations. In any case we have $\chi = 1 - g$, and G_I acts freely on vertices but not on edges, Case 2.

When $g > 1$ and $1 < I \mid 2g - 2$, take the above graph and the embedding $\rho : G_I \hookrightarrow G_{2g-2}$, $\sigma \mapsto \sigma^{\frac{2g-2}{I}}$. If I is odd, we are in Case 1; if I is even, Case 2.

⁵A real algebraic geometer might be tempted to point out that the graph naturally lives in the blowup of \mathbb{RP}^2 at a single point.

4. FURTHER REMARKS ON INDEX SPECIALIZATION

Consider first the case of a curve C/K admitting an R -model such that the *reduced subscheme* of the special fiber is semistable: such an arithmetic surface C/R is called an *SNC model* of its generic fiber C/K . It is known that every curve admits a regular SNC model. In this case, writing e_i for the multiplicity of C_i , the following simultaneous generalization of Theorem 9 and [8], [2] should hold:

$$(3) \quad I(C/K) = \gcd_i(d_i \cdot e_i \cdot I_i).$$

However, unlike the case of semistable reduction, it can happen even in the presence of (B) that there are two field extensions L_1, L_2 of K , with the same maximal unramified subextension and equal ramification indices $e(L_1/K) = e(L_2/K)$, and such that L_1 splits C but L_2 does not. So the determination of all splitting fields in the SNC case is fundamentally more complicated.

One may also consider the higher-dimensional context. One has the notion of a d -dimensional *semistable scheme* S/k : a reduced, finite-type k -scheme such that $S_{/\bar{k}} = \bigcup_i S_i$, where each S_i is connected, nonsingular, of dimension d , and whose singularities are analytically isomorphic to transversely intersecting hyperplanes. Suppose that S_i is minimally defined over l_i and put $d_i = [l_i : k]$. Let e_i be the multiplicity of S_i and I_i be the nonsingular index of $(S_i^{\text{red}})_{/l_i}$. Then define

$$I'(S/k) = \gcd_i(d_i \cdot e_i \cdot I_i).$$

If V/K is a (still smooth, projective, geometrically integral) variety over a Henselian discrete valuation field K , a *regular SNC-model* for V is a regular, flat R -scheme with generic fiber isomorphic to V and such that the reduced subscheme of the special fiber is semistable. It is apparently an open problem whether every variety V/K admits a regular SNC-model.

Conjecture 16. *Let V/K be a variety admitting a regular SNC-model, with special fiber $V_{/k}$. Then $I(V/K) = I'(V/k)$.*

Acknowledgements: I gratefully acknowledge financial support from MSRI and mathematical support from J.-L. Colliot-Thélène, D. Harbater, D. Lorenzini, Q. Liu, B. Poonen, S. Sharif and O. Wittenberg.

Added in revision, 5/2007: D. Lorenzini and Q. Liu have proved (3). Moreover, I am told they can prove Conjecture 16, at least conditionally on an extension of work of M. Levine – *Torsion zero-cycles on singular varieties*, Amer. J. Math. 107 (1985), no. 3, 737-757 – to the case of nonalgebraically closed k .

REFERENCES

- [1] M. Baker. *Specialization of linear systems from curves to graphs*, preprint, available at www.math.gatech.edu/~mbaker/pdf/specialization.pdf
- [2] S. Bosch and Q. Liu. *Rational points of the group of components of a Néron model*, Manuscripta Math. 98 (1999), 275-293.
- [3] P.L. Clark, *There are genus one curves of every index over every number field*, J. Reine Angew. Math 594 (2006), 201-206.
- [4] P.L. Clark, *On the Hasse principle for Shimura curves*, to appear in Israel J. Math.
- [5] P.L. Clark, *Abelian points on algebraic curves*, to appear in Math. Research Letters.
- [6] P.L. Clark and S.I. Sharif, *Period, index and potential III*, in preparation.

- [7] J.-L. Colliot-Thélène, *Un théorème de finitude pour le groupe de Chow des zéro-cycles d'une groupe algébrique linéaire sur un corps p -adique*, Invent. math. 159 (2005), 589-606.
- [8] J.-L. Colliot-Thélène and S. Saito, *Zéro-cycles sur les varités p -adiques et groupe de Brauer*, International Mathematical Research Notices 1996, n. 4, 151-160.
- [9] M. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik (3) 11 (1986), Springer-Verlag.
- [10] P. de la Harpe. *Topics in Geometric Group Theory*, University of Chicago Press, 2000.
- [11] B.W. Jordan and R. Livné. *Local diophantine properties of Shimura curves*, Math. Ann. 270 (1985), 235-248.
- [12] A. Pál. *Solvable points on projective algebraic curves*, Canad. J. Math. 56 (2004), 612-637.
- [13] B. Poonen and M. Stoll. *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. 150 (1999), 1109-1149.
- [14] J.-P. Serre. *Corps Locaux*, Hermann, Paris, 1962.
- [15] S.I. Sharif. *Construction of curves with prescribed period and index*, 2006 Berkeley thesis.
- [16] A. Vistoli. *The deformation theory of local complete intersections*, [arXiv:math.AG/9703008](https://arxiv.org/abs/math/9703008).
- [17] E. Witt. *Über ein Gegenispiel zum Normensatz*, Math. Z. 39 (1934), 462-267.

DEPARTMENT OF MATHEMATICS, BOYD GRADUATE STUDIES RESEARCH CENTER, UNIVERSITY OF GEORGIA, ATHENS, GA 30602-7403, USA

E-mail address: pete@math.uga.edu